RDMAttack! or how I learned to stop worrying and authenticate at line rate

Stew, Shu-Ting, Yibo
University of California San Diego

Figure 1: My goodness this is a fantastic figure, it's so nice it could probably be used at a template for future figures.

RDMA Variant	Sec prop	Verbs	Attack
RC	Seq Num	Read, Write, Send, Rec	Spoofing Seq
UC		Read, Send, Rec	Read
UD	Queue Pain Key	Send, Rec	

Table 1: A table roughly describing RDMA security primitives

1 Abstract

RDMA is growing in popularity and it's adoption is slowly growing beyond the secure world of the data centre. As a high throughput protocol RDMA was never designed with security in mind and is open for attacks.

In this work we review prior work on securing RDMA, *Demonstrate that current proposed security protocols such as TLS and RDMA specific security cannot scale to 100Gb networking*. Demonstrate that RDMA traffic can be hijacked using a trivial man in the middle attack, and propose high throughput security primitives for securing RDMA.

2 Introduction

3 Background

- TLS
- RoCE
- Iwarp
- Secure RDMA

4 Experimental Setup

5 Evaluation

Here we hijack an RDMA session and learn *secret* data from a the remote memory of an unsuspecting server. Then using a similar but slightly modified version of the attack we inject write verbs and demonstrate that we can easily write to exposed RDMAable memory. Figure 1 is an example of what a figure can be.

6 Conclusion

All of our work should be encorporated into RoCEv3

References